THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A digital private key protection device, comprising

a digital private key storage means containing a user's digital private key;

a cryptographic engine;

a communications port for receiving digital data from an external device, and for transmitting data to said external device;

a display means for displaying said received digital data;

a user operable input means connected to said cryptographic engine to indicate when operated by said user their approval of said displayed received digital data; wherein

said cryptographic engine is trusted to only apply said user's digital private key to sign said received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device .

2. A digital private key protection device according to claim 1, wherein said digital key storage means contains a trusted public key and a plurality of user's public keys signed by said trusted private key; and said cryptographic engine validates signature of said user's public key with said trusted public key to determine the veracity of said user's public key and then decrypts said received data using said verified predetermined user's public key and causes said display to indicate whether said user's private key was used to sign said received digital data.

Sub a4

3. A private key protection system according to claims 1 and 2 wherein said signed digital data is a digital certificate.

4. A private key protection system according to claim 1 further comprising an audit means wherein signed data is not transmitted external of said digital private key protection device until a said encryption process is audited by said audit means.

5. A private key protection system according to claim 2 further comprising an audit means wherein signed data is not displayed until a said encryption process is audited by said audit means.

6. A private key protection system according to claim 1 wherein said digital private key protection device further comprises a private key protection device private key storage means wherein digital data signed by said private key protection device after operation of said user operable input means is further signed by said private key of said private key protection device.

7. A digital private key protection device according to claim 1 wherein said digital key storage means contains a predetermined digital private key protection device's public key; such that when said communications port receives signed digital data from an external device which may or may not have been signed by a said predetermined digital private key protection device;

said cryptographic engine decrypts said received data using said predetermined digital private key protection device's public key to verify whether said digital private key protection device's private key was used to sign said received data.

8. A digital private key protection device according to claim 7 wherein said display means indicates whether said digital private key protection device's private key was used to encrypt said received data.

9. A digital private key protection device according to claim 1 further comprising a public key storage means containing a plurality of user's public keys; and

said received digital data contains information that predetermines which user's public key is used to sign said received data that is transmitted external of said digital private key protection device to said predetermined user.

10. A digital private key protection device according to claim 1 wherein said cryptographic engine is trusted to decrypt digital data using said user's digital private key and passing decrypted digital data to said display means for display of said received digital data.

11. A digital private key protection device according to claim 10 wherein said cryptographic engine does not decrypt signed digital data unless said user operable input means is operated.

12. A digital private key protection device according to claim 10 wherein said communications port can not transmit said decrypted digital data.

13. A digital private key protection device according to claim 12 wherein said communications port can not transmit said decrypted digital data unless said user operable input means is operated.

14. A digital private key protection device according to claim 1 wherein said digital private key storage means also contains a digital shared secret symmetric key wherein said cryptographic engine is trusted to only apply said digital shared secret symmetric key to encrypt data only if said user operable input

means is operated and also trusted to communicate said signed data external of said digital private key protection device.

Sub a5

15. A digital private key protection device according to any preceding claim wherein said received digital data contains an instruction which determines how said encryption engine should encrypt or decrypt respectively.

16. A digital private key protection device according to any preceding claim wherein said received digital data contains an instruction which determines which protocol is used by said device to communicate encrypted or signed data external of said device.

17. A digital private key protection device according to any preceding claim wherein said display means is external to said device and controlled by said device for displaying data transmitted from said communications port.

18. A digital private key protection device according to any preceding claim wherein said user operable input means is external to said device and controlled by said device to be actuated by said user in a predetermined manner.

19. A digital private key protection device according to any preceding claim further comprising identification and authentication means actuated by said user in a predetermined manner.

20. A digital private key protection device according to claim 18 further comprising an audit means which audits said actuation of said user identification input means.

Sub a6

21. A digital private key protection device according to any preceding claim wherein said digital private key storage means is removable from said device.

22. A digital private key protection device according to any preceding claim wherein a cryptographic request is received from said external device according to a predetermined application programming interface, such that the request is performed by said PKPD using the user's private or other keys as identified by the request, but excluding the private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined.

23. A digital private key protection device according to claim 22 wherein said device displays a description of said request to the user and, only if the user operates said user operable input means, does said device carry out said request.